DII.COE.Final.HP1020.IP

Defense Information Infrastructure (DII)

Common Operating Environment (COE)

Installation Procedures (IP) for SPI, version 1.0.0.2

Document Version 1.0.0.2

27 August 1997

Prepared for:

Defense Information Systems Agency

Prepared by:

NRaD
San Diego, CA

Table of Contents

This page intentionally left blank.

1. Scope

1.1 Identification

This Installation Procedures Document describes the installation procedures for SPI (segprefix SPI322) Version 1.0.0.2 for the HP 10.20 Platform.

1.2 System Overview

This version of SPI-NET provides the capability to conduct simultaneous inspections of the UNIX hosts of a security domain from a central control point called the Command Center. Inpsections may be performed on demand, and may also be scheduled to run automatically on a regular basis.

2. Referenced Documents

System Administrator's Manual (SAM) for SPI version 1.0.0.2, 27 August 1997.

3. System Environment

3.1 System Requirements

3.1.1 Hardware Requirements

None.

3.1.2 Operating System Requirements

The HPUX 10.20 Operating System is required to perform the installation of SPI 1.0.0.2.

3.1.3 Kernel Requirements

DII COE Kernel Version 3.0.1.0 is required to perform the installation of SPI 1.0.0.2.

3.2 System and Site Preparations

3.2.1 System Configuration

None.

3.2.2 Operating System Preparation

Log into the HP10.20 system as "sysadmin." After the system loads, go to the pull down menu labeled Software and select Segment Installer. This activates the COEInstaller.

3.2.3 Tape/Disk Preparation

Once the COEInstaller has been activated, choose the Select Source button to identify the source/location of the segment. When this window appears, select Other, then type in the location of your 8mm exabyte drive (which usually is /dev/rmt/0mn). Then choose OK.

4. Installation Instructions

4.1 Media Booting Procedures

None.

4.2 Installation Procedures

After completing paras 3.2.2 and 3.2.3 above, choose Read Contents in the Installer window to list the segments on the selected drive. The SPI 1.0.0.2 segment will appear. Highlight the segment, then choose the Install button. This will install the SPI segment into the /h/COE/Comp directory.

Make sure to execute instructions from Section 4.5 Initializing the Software.

4.3 Installation of Upgrades

None.

4.4 Installation Verification

To verify that the segment has been installed, go to the /h/COE/Comp directory to see if you see a SPI directory. If so, the segment has been installed. Within the COEInstaller API, you can view the "Installation log" to verify "successfull installation."

4.5 Initializing the Software

During installation, you will be required to ok many questions. One question is particularly important. When prompted to insert the address of the host system, you have two choices: 1)Insert the full address (ex. diicoe23.nosc.mil) ro 2)insert the name of the system (ex. falcon). If you insert the incorrect name, you will receive errors while running SPI, and will have to reinstall the segment correctly for it to run properly.

After installation, the StartRCS file within /h/COE/Comp/SPI322/bin/spin-97.06A/binr is required to run SPI. This file should be running continuously, unless it has been halted. To verify that it is running, log into an xterm window as root. Type ps -ef | grep "*rcs*". This will find all processes that contain "rcs." If one is found under /h/../spin-97.06A/binr, then the process is running. If not, just type "cd /h/COE/Comp/SPI322/bin/spin-97.06A/binr", then type "./StartRCS" to activate this file.

4.6 List of Changes and Enhancements

This version contains the conversion of SPI from a COTS segment into a COE Component software segment.

4.7 Important Considerations

None.

5. Notes

It is a known problem that if you use the COEInstaller from a command line with the debug option (-d) that some segments will not install/deinstall. The workaround for this problem is to type 'setenv DISPLAY unix:0.0' at the sysadmin prompt before trying to launch the installer.

Appendix A

SPI-NET Installation Overview

Topics:

1. Overview of the SPI-NET Distribution Content
2. System requirements for SPI-NET Operation
3. Installing the SPI-NET Command Center
4. Defining the SPI-NET Security Domain
5. Installing SPI-NET Remote Inspection Systems

1. Overview of the SPI-NET Distribution Content:

The SPI-NET distribution package will create a directory "spin-(version)".

All SPI-NET source files will be placed within this directory, (as will the final executables and datafiles, unless you override during install.)

The major distribution components (in the directory spin-(version)) are:

(master source code distribution)

```
MANIFEST        File listing for the entire SPI-NET distribution
  Help/         Hierarchy of SPI-NET Help files
Install*        Installs entire SPI-NET system for Commandhost
                (includes local install of Remote Inspection System)
Configure*      (used by Install)
Makefile.SH     (used by Install)

MANIFEST_R      File listing for the remote SPI-NET distribution
Installr*       Installs remote SPI-NET system for target host(s)
Config_R*       (used by Installr)
Makefile_R.SH   (used by Installr)

Snapshot.SH     (used by Install and Installr)
config.h.SH     (used by Install and Installr)
include/        C header files for all sources
man/            UNIX-style manual pages for SPI-NET executables
srcl/           Source code for various SPI-NET libraries
srcm/           Source code for SPI-NET Command Center executables
srcr/           Source code for SPI-NET Remote Inspection System
  tcltk/        Source code for Tcl and Tk GUI interpreters
```

(remote source code distribution)

```
MANIFEST_R      File listing for the remote SPI-NET distribution
Installr*       Installs remote SPI-NET system for target host(s)
Config_R*       (used by Installr)
Makefile_R.SH   (used by Installr)

Snapshot.SH     (used by Install and Installr)
config.h.SH     (used by Install and Installr)
include/        C header files for all sources
man/            UNIX-style manual pages for SPI-NET executables
srcl/           Source code for various SPI-NET libraries
srcr/           Source code for SPI-NET Remote Inspection System
```

(master binary distribution)

```
MANIFESTB       File listing for the binary SPI-NET distribution
```

```
SetUp*          Binary environment configuration script
Snapshot*       Manual CDT Baseline creation (optional)
man/           UNIX-style manual pages for SPI-NET executables
binm/          Command Center Executables and Data Directory
binr/         Remote-side Executables and Data Directory
  tcltk/        Tcl/Tk GUI interpreters and libraries
```

(remote binary distribution)

```
MANIFESTB_R     File listing for the remote-side binary distribution
SetUp*          Binary environment configuration script
Snapshot*       Manual CDT Baseline creation (optional)
man/           UNIX-style manual pages for SPI-NET executables
binr/         Remote-side Executables and Data Directory
```

2. System requirements for SPI-NET Operation

The SPI-NET Command Center will employ an Xwindows-based graphical user interface. While SPI-NET provides the tcl/tk widgets and code, it will not supply the underlying Xwindows libraries. These libraries (X11) must be present in order to build the SPI-NET User Interface.

(It is possible, though not convenient, to run the SPI-NET Command Center via supplied scripts.)

The Remote Inspection System needs only the standard UNIX utilities.

3. Installing the SPI-NET Command Center:

When you build a complete SPI-NET (via the Install script) ALL of the above codes are compiled and installed on the local system (generally referred to as the CommandHost). This includes the remote inspector tools and the remote communications agents. This way, self-inspection of the local system occurs just as if it were another remote inspection target.

By default, all of the CommandHost executables and datafiles will be placed in the directory "spin-(version)/binm/" and a local copy of the remote inspection system executables are placed in "spin-(version)/binr".

```
========================
SOURCE CODE INSTALLATION
========================
```

To do a source install of the entire SPI-NET package on the CommandHost, run the Install script provided in the original tar directory.

```
% ./Install
```

The installation will proceed in four parts:

A. Configuration (asks a few questions, provides default answers)
B. Compilation/Installation
C. Snapshot for CDT database (optional, may be deferred)

Creating/Updating a Production Environment (source package only)

During SPI-NET (source code) configuration, you will be asked if you wish to create a production environment. If you answer "yes", then after SPI-NET is completely compiled and installed, four tar files will be created and placed in the directory that you specify. These four files will be:

a. A new spinS full source package.
b. A new spinRS remote-only source package.
c. A new spin.b full binary package (platform specific).
d. A new spin.rb remote binary package (platform specific).

These packages can be recreated anytime you give the command "make product" in the master source directory, or by giving the "Install -s" command to the top-level Install script.

==========
BINARY CODE INSTALLATION
==========

To do a binary install of the entire SPI-NET package on the Command host, type

```
% ./SetUp
```

The installation will proceed in three parts:

A. Configuration (asks a few questions)
B. Installation
C. Snapshot for CDT database (optional, may be deferred)

4. Defining the SPI-NET Security Domain

NOTE: If you do not intend to inspect remote host systems, you may proceed directly to the document "Help/Documentation/Operations". (Source for Help documents is located in the main install directory.)

Most of what follows is performed automatically by the master and remote Install or SetUp scripts. Additional elements can be set through the user interface on the Command Center. However, if you wish to manually check these elements, they are described below.

A. Assignment of SPI-NET Host Identifiers (HostIDs)
B. Generation and Distribution of DSS certificates

The first is to check (binm or binr)/D/HOSTINFO/Host_Table on each of the remote hosts of the security domain to establish their SPI-NET HostIDs. The second is to distribute the generated private-key certificates to the D/CERTINFO directory in each remote host. The third (actually an element of "Operations") is to start-up the RCS server(s).

All of these tasks will refer to elements found in or below the directory spin-(version)/binm, and the remainder of this discussion will assume that that this is the current directory.

A. Assigning HostIDs

The SPI-NET system references all host machines in terms of a HostID of the form "HID_nnnnnn". By default, the CommandHost has already been assigned the HostID "HID_000001". If your hostname is, say, "wildcard", then the file "D/HOSTINFO/Host_Table" should already contain the line

HID_000001:wildcard

To add the hosts "ace", "king" and "queen" to the Host_Table, you need to select arbitrary ID numbers (padded to 6 digits) and write them to this file, E.G.:

```
HID_000001:wildcard.wsu.edu  (or)   HID_000001:wildcard
HID_000002:ace.wsu.edu              HID_000202:ace
HID_000003:king.wsu.edu             HID_000203:king
HID_000004:queen.wsu.edu            HID_000207:queen
```

(Later, when installing SPI-NET Remote on each of these target systems, there will be a corresponding directory and file "Host_Table" that must

contain these entries, or at least the subset need for communication.
For example, "king" would need the entries for "king" and "wildcard".)

Defining HostGroups

NOTE: This operation may be performed entirely through the SPI-NET user interface. The manual procedure is described here.

HostGroups are arbitrary subsets of hosts from the security domain. They are created for several reasons, but the primary reason is to aid in defining inspection jobgroups and schedules.

The directory "D/HOSTGRPS" should already contain two files. These are

COMMANDHOST and ALLHOSTS

At present, each file should contain the word HID_000001 on a single line. Continuing with the above example, you should edit the file ALLHOSTS so that it contains the lines

HID_000001	(or)	HID_000001
HID_000002		HID_000202
HID_000003		HID_000203
HID_000004		HID_000207

You may create arbitrary subsets of hosts by creating additional files. The chosen filename becomes the name of the new HostGroup, and its members are defined by the HostIDs contained in that file. By placing only a single HostID in a file, that HostGroup becomes a SPI-NET alias for the indicated target host.

There are no corresponding HostGroup files to be installed for the remote inspection targets.

B. Generation and Distribution of DSS certificates

NOTE_1: The DSS "certificates" referenced herein are primitive and prototypical, based upon the NIST DSSFIPS document. They are written in an entirely ASCII format, with numerical values represented in pairs of hexadecimal characters. They support the required mathematical functionality as specified in the standard, but they carry no internal information in support of hierarchical certificate issuing authorities, certificate revocation lists (CRLs) etc. Management of the certificates rests solely with the SPI-NET operator. This document is intended as a guide to the management of certificates.

NOTE_2: For stand-alone operation, all DSS key certificates needed for local SPI-NET operation have already been created and distributed. However, it is important to understand this process in order to form additional certificates, even if only to renew the local ones, which should be done on a semi-annual basis (or in the event that the system has been compromised,) in order to maximize security assurance. Although the certificate you now have was based on a "certificate master" that is common to all SPI-NET 0.9x distributions, your local UNIX time was used as a seed to randomize the public and private key prime generation, and insure that your key values are unique.

Generation of DSS certificates involves generation of several prime numbers, some of which are rather large. This process is cpu-time-intensive. Fortunately, once the large primes are established, it is possible to quickly create a virtually limitless (and if desired, randomly seeded) array of certificates. For reasons of efficiency, we have provided three separate modules for the out-of-band generation and use of DSS certificates. These are:

dss_GenMaster - Create or update a certificate master

dss_GenCerts - Create multiple certificates based upon a master

dss_Signature - Supports manual signing or verification of files

For the purpose of SPI-NET operations, only dss_GenCerts (and the file binm/D/CERT_DB/dist_certmaster supplied with the distribution) is needed to supply the system with future certificates. The module dss_GenMaster is provided in case the dist_certmaster is somehow lost, or for those who wish to create an entirely fresh "family" of certificates. Also, the SPI-NET clients and servers conduct built-in DSS signing, verifying, and optional DES encrypting of data transmissions, based upon codes similar to those in dss_Signature. The module dss_Signature is provided for demonstration purposes, and for optional digital signature generation and verification outside of SPI-NET operations.

Detailed use of all three DSS-based modules is described in the man pages (spin)/binm/man/man8/dss.8 that are supplied with the distribution. The following overview is intended more to assist in understanding the generation of new certificates, and how these must be distributed for operation of SPI-NET remote inspections.

Generating Additional DSS Certificates for Distributed SPI-NET Operation:

Assume that, in addition to the SPI-NET Command Host, you intend to inspect the systems "ace", "king", and "queen". You will need to create three additional certificates. Place yourself in the directory named "binm/D/CERT_DB" and issue the command

```
../../dss_GenCerts -N 3 dist_certmaster
```

This will create three new certificates in the form of three pairs of files, named

```
crt_000002.prv      crt_000003.prv      crt_000004.prv
crt_000002.pub      crt_000003.pub      crt_000004.pub
```

(The file dist_certmaster maintains the certificate ID of the last generated certificate, and defaults to naming new certificates by incrementing this number. This can be overridden with the -C option. E.G., dss_GenCerts -C 205 ... would have created crt_000205, crt_000206, and crt_000207)

Note that certificate pairs have extensions "prv" and "pub". These are the PRIVATE and PUBLIC forms of the certificate. The only real difference is that PRIVATE component contains a large secret key, unique to that certificate, that is not part of the PUBLIC component.

If you had earlier assigned the hosts ace, king and queen the SPI-NET HostIDs HID_000002, HID_000003, and HID_000004, then the HostIDs would match the 6-digit portion of the certificate names, and you would be ready distribute the certificates. If instead, "ace" was given the HostID "HID_222345" then you would need to rename the certificate to have the matching 6-digit portion, crt_222345. (The certificates maintain their original CERT_IDs internally for reference purposes.)

Distribution of certificates is dictated by the following two rules:

a. Each host is the sole "owner" of its PRIVATE component.
b. Each host needs a copy of the PUBLIC component of each host that it will need to communicate with.

Since SPI-NET operation is "one-to-many" (one CommandHost, many Remote Inspection Targets) and only communication between a remote host and the CommandHost is supported, it follows that

a. The CommandHost needs its PRIVATE component, and the PUBLIC component from all other hosts, as it needs to communicate with each one.
b. Each RemoteHost needs its PRIVATE component, and the PUBLIC component

from the CommandHost.

Each SPI-NET host has a directory "D/CERTINFO" where the operational certificates must reside. For the above example, where CommandHost, ace, king, and queen are 000001, 000002, 000003, and 000004, these directories would need to contain the following:

CommandHost	ace	king	queen
crt_000001.prv	crt_000002.prv	crt_000003.prv	crt_000004.prv
crt_000001.pub	crt_000001.pub	crt_000001.pub	crt_000001.pub
crt_000002.pub			
crt_000003.pub			
crt_000004.pub			

(Note that the CommandHost needs its own crt_000001.pub so that it can conduct "remote" inspections of itself.)

The SPI-NET Remote Distribution Package spin-0.9x.tar.Z, being produced after the CommandHost installation, will already contain the default CommandHost PUBLIC certificate crt_000001.pub, and will automatically place this certificate in the remote (binr)D/CERTINFO directory.

To complete the preparations for the Remote Inspection System install, you will only need to create the addition certificates, place all the PUBLIC components into the binm/D/CERTINFO directory of the CommandHost, and eventually move each PRIVATE component to its owner host.

For detailed use of the DSS-based certificate modules, see the man pages (spin)/binm/man/man8/dss.8 that are supplied with the distribution.

5. Installing the SPI-NET Remote Inspection System

NOTE_1: If you do not intend to inspect remote host systems, you may proceed directly to the document "Help/Documentation/Operations".

NOTE_2: Prior to operation of SPI-NET remote inspections, you will need to define Host IDs for the hosts in the intended security domain, and to create DSS key certificates for each of the remote inspection targets. (For the CommandHost, this has already been done automatically by Install.) Details on certificate generation are provided above in part 4B.

The SPI-NET Remote Distribution Package installation is very similar to installation on the CommandHost. The "spin_r-(version).Z" package will create a directory called "spin_r-(version)" and will place all of the

Remote Distribution source files in this directory.

The directory should contain the following:

```
MANIFEST_R      File listing for the remote SPI-NET distribution
Installr*       Installs remote SPI-NET system for target host(s)
Config_R*       (used by Installr)
Makefile_R.SH   (used by Installr)

Snapshot.SH     (used by Install and Installr)
config.h.SH     (used by Install and Installr)
include/        C header files for all sources
man/            UNIX-style manual pages for SPI-NET executables
srcl/           Source code for various SPI-NET libraries
srcr/           Source code for SPI-NET Remote Inspection System
```

By default, all of the remote host executables and datafiles will be placed in the directory "spin-(version)/binr/".

To do a source install of the remote SPI-NET package on a given host, run the Installr script provided in the original tar directory.

```
% ./Installr
```

The installation will proceed in three parts:

A. Configuration (asks a few questions, provides default answers)
B. Compilation/Installation
C. Snapshot for CDT database (optional, may be deferred)

To do a binary install of the remote SPI-NET package on a given host, run the SetUp script located in the spin-(version) directory.

```
% ./SetUp
```

The installation will proceed in three parts:

A. Configuration (asks a few questions)
B. Installation
C. Snapshot for CDT database (optional, may be deferred)

As mentioned above, you must do two more things to prepare for SPI-NET remote host inspections:

First, you should check the file (binr)/D/HOSTINFO/Host_Table. It should

already contain the two lines

HID_000001:command_host_name
HID_nnnnnn:local_host_name

where command_host_name is the standard hostname of the machine that will be serving in the role of the SPI-NET CommandHost. These two lines should have been created by running the SetUp script.

Second, you must install a DSS PRIVATE key certificate for this host. The directory (binr)/D/CERTINFO should already contain the PUBLIC certificate of the CommandHost, crt_000001.pub. You must add to this directory the PRIVATE certificate corresponding to this host's SPI-NET HostID. If this remote host is designated HID_000204, then the CERTINFO directory must contain the PRIVATE certificate crt_000204.prv.

A more complete description of SPI-NET HostID assignment and certificate distribution is given in part 4 above.

Once you have completed all of the activities listed above, you can begin to apply the instructions in "Help/Documentation/Operations".

This page intentionally left blank.